Sumário Executivo para as Recomendações

Projeto Revisão do Modelo de Transporte de Ônibus do Rio de Janeiro

Etapa 2 - Auditoria do Sistema de Bilhetagem Eletrônica (SBE)

pwc strategy&

(DC2) Uso Restrito na PwC - Confidencial

Índice

1. ***Recomendações para o relatório P04 – Relatório de Avaliação das Regras de Negócio (baseadas em leis e legislações vigentes)***
2. ***Recomendações para o relatório P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica***
3. ***Recomendações para o relatório P06 – Relatório de Funcionalidades***

(DC2) Uso Restrito na PwC - Confidencial

1

Recomendações para o relatório P04 – Relatório de Avaliação das Regras de Negócio (baseadas em leis e legislações vigentes)

(DC2) Uso Restrito na PwC - Confidencial

Recomendações: P04 – Relatório de Avaliação das Regras de Negócio

1. É recomendado a revisão de todas as transações apresentadas para identificar a origem do não cadastramento desses cartões na base de dados do Sistema de Bilhetagem Eletrônica (SBE), bem como a avaliação se os cartões são efetivamente válidos ou devem ser cancelados;
2. É recomendado uma verificação detalhada das transações apresentadas com exceções com o objetivo de identificar se os portadores dos cartões são de fato elegíveis ao benefício de gratuidade e habilitar apenas um cartão de gratuidade para cada usuário;
3. É recomendado que seja implementado um controle automático de verificação de CPFs cadastrados, com o objetivo de impedir que o mesmo CPF seja cadastrado mais de uma vez para emissão de cartões adicionais de gratuidade;
4. É recomendado que no processo de cadastramento do CPFs possua funções para validação do digito verificador;
5. É sugerido uma revisão completa dos CPFs cadastrados na base de usuários de cartões;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações: P04 – Relatório de Avaliação das Regras de Negócio (cont.)

6. É recomendado que seja implementado controles que possam garantir o cancelamento dos cartões de gratuidade de forma tempestiva, e que seu uso seja efetivamente impossibilitado;

7. É recomendado que sejam implementados controles de validação antes da concessão do benefício, visando garantir que o benefício será concedido apenas para pessoas elegíveis;

8. É recomendado revisar periodicamente a base cadastral de gratuidades com o propósito de identificar casos de não elegibilidades e tomar as ações necessárias;

9. Implementar controles para não permitir a criação de usuários de teste em ambiente produtivo;

10. É recomendado que sejam implementados controles que limitem a utilização máxima do benefício de gratuidade para estudantes para 4 (quatro) viagens por dia respeitando o que foi estabelecido no Decreto N° 38280/14;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P04 – Relatório de Avaliação das Regras de Negócio (cont.)

11. É recomendado que seja implementado um controle periódico onde a SMTR, através de convênio com a Dataprev, forneça a relação de registros de óbitos à RioCard, para que o Sistema SBE seja sensibilizado de forma a cancelar os cartões associados aos CPFs com registro de óbito;

12. Apesar da sincronização dos relógios dos validadores estarem prevista no processo de atualização do validador, recomendamos que seja adotado um controle para garantir que os horários sejam sincronizados de forma efetiva e tempestiva para a totalidade dos validadores;

13. Um controle detectivo de horários incorretos de validadores deve ser implementado no momento do processamento das transações, de modo a identificar as não conformidades e estabelecer a abertura de um incidente demandando a posterior atualização do validador;

14. É recomendado que sejam implementados controles para garantir que a quantidade mínima de integrações diárias seja respeitada;

15. É recomendado que a RioCard acompanhe a resolução do chamado garantindo que a causa raiz (origem) do problema seja identificada e corrigida;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P04 – Relatório de Avaliação das Regras de Negócio (cont.)

16. É recomendado que a RioCard monitore a resolução dessa situação junto às empresas de ônibus, bem como crie procedimentos de atualização das versões de sistemas, evitando transtornos de contestação decorrentes de não reconciliação dos valores processados e presentes nas filipetas;

17. Implementar controles, como de assinatura digital baseada em chave pública-privada, para garantir a privacidade e autenticidade dos arquivos, listados anteriormente, gerados no Sistema de Bilhetagem Eletrônica (SBE) e enviados ao Validador;

18. Implementar controles automatizados sobre a realização da carga diária nos validadores, que inclua registros das execuções e exceções em logs, bem como sejam capazes de garantir a totalidade e integridade dos arquivos enviados.

(DC2) Uso Restrito na PwC - Confidencial

2

Recomendações para o relatório P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica

1. É recomendado que se use restrição de permissão (ACLS) para impossibilitar leitura anônima dos arquivos/pastas e também para não permitir o acesso e alteração a informações restritas da aplicação web;
2. É recomendado que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso;
3. É recomendado que as informações sensíveis sejam trafegadas por conexões criptografadas (HTTPS) para que os dados não sejam interceptados por um usuário malicioso;
4. É recomendado a avaliação da necessidade de se ter a possibilidade de se listar arquivos e de garantir de que esses arquivos não exponham informações que possam ser utilizadas por usuários mal intencionados;
5. É recomendado que não seja habilitada a possibilidade de listagem de diretórios nas configurações do web server;
6. É recomendado utilizar como medida de prevenção a implementação e inclusão de tokens na sessão (atual) de um usuário (Tokens são valores criptográficos longos que são difíceis de adivinhar);

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica (cont.)

7. Tokens serão gerados quando a sessão de um usuário começar e será associada com a sessão deste usuário em particular;
8. Esse challange token será incluído em cada solicitação, que será usado pelo lado do servidor para verificar a legitimidade da requisição do usuário final;
9. É recomendado que a verificação do CAPTCHA deva ser feito no servidor sem ser exposto ao lado cliente da comunicação;
10. A causa da vulnerabilidade pode depender de aplicação para aplicação, uma análise mais profunda deve ser realizada para a correção do problema;
11. É recomendado entrar em contato com o responsável pela aplicação para a correção do problema;
12. É recomendado utilizar como medida de prevenção a implementação e inclusão de tokens na sessão (atual) de um usuário;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica (cont.)

13. Esse challange token será incluído em cada solicitação, que será usado pelo lado do servidor para verificar a legitimidade da requisição do usuário final;
14. É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options;
15. É recomendado se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção;
16. É recomendado verificar a possibilidade de se habilitar o HTTPOnly para aprimorar a proteção dos cookies de sessão de sua aplicação;
17. É recomendado colocar a Secure flag para esse cookie;
18. É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options;
19. É recomendado se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção;
20. É recomendado verificar a possibilidade de se habilitar o HTTPOnly para aprimorar a proteção dos cookies de sessão de sua aplicação;
21. É recomendado colocar a Secure flag para esse cookie;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica (cont.)

22. É recomendado configurar seu servidor web para incluir um cabeçalho X-frame-Options;
23. É recomendado se desabilitar todos os métodos não necessários e de desenvolvimento para sites de produção;
24. Desativar o Modo Agressivo, se suportado;
25. Não usar chave pré-compartilhada para autenticação, se possível;
26. Se estiver usando chave pré-compartilhada, usar senhas fortes;
27. Se possível, não permita conexões VPN para certos endereços IP;
28. É recomendado avaliar se é necessário instalar um novo certificado assinado por uma autoridade certificadora;
29. É recomendado avaliar se é necessário instalar um novo certificado assinado por uma autoridade certificadora;
30. É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P05 – Relatório de Segurança do Sistema de Bilhetagem Eletrônica (cont.)

31. Verificar a possibilidade de inserir um endereço de email genérico com domínio corporativo, por exemplo: segurança@riocard.com;
32. É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet;
33. Verificar a possibilidade de inserir um endereço de email genérico com domínio corporativo, por exemplo: segurança@riocard.com;
34. É recomendado que nenhuma informação particular de funcionários ou prestadores de serviços seja exposta publicamente na internet;
35. Verificar a possibilidade de inserir um endereço de email genérico com domínio corporativo, por exemplo segurança@riocard.com.

(DC2) Uso Restrito na PwC - Confidencial

3

Recomendações para o relatório P06 – Relatório de Funcionalidades

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P06 – Relatório de Funcionalidades

1. É Recomendado a implementação de um controle no SBE que possibilite a identificação de transações realizadas com cartões que não constam na base de cartões ativos do SBE, gerando um registro de incidente a ser tratado;
2. É Recomendado que o CPF seja utilizado como campo chave nos registros, facilitando a revisão da base para garantir que cada usuário tenha apenas um cartão;
3. É Recomendado a realização de uma verificação periódica, para os cartões que realizaram transações de gratuidade e não estão na base cadastral, com o objetivo de identificar se os usuários desses cartões são de fato elegíveis ao benefício;
4. Para os casos onde os usuários são elegíveis, é necessário cadastra-los. E para os casos onde os usuários não são elegíveis, o benefício deve ser revogado;
5. É Recomendado que seja implementado controles de validação antes da concessão do benefício, visando garantir que o benefício será concedido apenas para pessoas elegíveis;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P06 – Relatório de Funcionalidades (cont.)

6. É recomendado revisar periodicamente a base cadastral de gratuidades com o propósito de identificar casos de não elegibilidades e tomar as ações necessárias;

7. É recomendado que seja implementado um controle periódico onde a SMTR, através de convênio com a Dataprev, forneça a relação de registros de óbitos à RioCard. Para que esta sensibilize o sistema SBE de forma a cancelar os cartões associados aos CPFs com registro de óbito;

8. É recomendado que sejam implementados controles que possam garantir o cancelamento dos cartões de gratuidade de forma tempestiva, e que seu uso seja efetivamente impossibilitado;

9. É recomendado a realização de uma verificação periódica, com o objetivo de identificar se os portadores desses cartões são, de fato, elegíveis ao benefício de gratuidade, habilitando apenas um cartão de gratuidade para cada usuário;

10. É recomendado que seja implementado um controle automático de verificação de CPFs cadastrados, com o objetivo de impedir que o mesmo CPF seja cadastrado mais de uma vez para emissão de cartões adicionais de gratuidade;

(DC2) Uso Restrito na PwC - Confidencial

Recomendações : P06 – Relatório de Funcionalidades (cont.)

11. É recomendado que o sistema onde são cadastrados os CPFs possua a função para validação do digito verificador, com o objetivo de fornecer um nível maior de confiabilidade das informações cadastradas;

12. É recomendado a implementação de controles para garantir o registro e análise da integridade dos arquivos originados no SBE e enviados ao validador;

13. É recomendado a elaboração de controles como: Assinatura Digital baseada em chave pública/privada, para garantir a autenticidade dos arquivos (Ex.: EOD, LIN, ITG, lista de recargas e hotlists) gerados no SBE e enviados ao Validador.

(DC2) Uso Restrito na PwC - Confidencial

Obrigado!

www.pwc.com.br
&
www.strategyand.pwc.com

© 2015 PricewaterhouseCoopers Corporate Finance & Recovery Ltda. Todos os direitos reservados. Neste documento, “PwC” refere-se à PricewaterhouseCoopers Serviços Profissionais Ltda, a qual é uma firma membro do network da PricewaterhouseCoopers International Limited, sendo que cada firma membro constitui-se em uma pessoa jurídica totalmente separada e independente.

O termo “PwC” refere-se à rede (network) de firmas membro da PricewaterhouseCoopers International Limited (PwCIL) ou, conforme o contexto determina, a cada uma das firmas membro participantes da rede da PwC. Cada firma membro da rede constitui uma pessoa jurídica separada e independente e que não atua como agente da PwCIL nem de qualquer outra firma membro. A PwCIL não presta serviços a clientes. A PwCIL não é responsável ou se obriga pelos atos ou omissões de qualquer de suas firmas membro, tampouco controla o julgamento profissional das referidas firmas ou pode obrigá-las de qualquer forma. Nenhuma firma membro é responsável pelos atos ou omissões de outra firma membro, nem controla o julgamento profissional de outra firma membro ou da PwCIL, nem pode obrigá-las de qualquer forma.

(DC2) Uso Restrito na PwC - Confidencial